

1 CHRISTOPHER CHORBA (SBN 216692)
cchorba@gibsondunn.com
2 TIMOTHY W. LOOSE (SBN 241037)
tloose@gibsondunn.com
3 TIAUNIA BEDELL (SBN 254323)
tbedell@gibsondunn.com
4 CHRISTINA YANG (SBN 300387)
cyang@gibsondunn.com
5 GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
6 Los Angeles, CA 90071-3197
Telephone: (213) 229-7000
7 Facsimile: (213) 229-7520

8 *Attorneys for Defendants Toyota Motor Corporation*
9 *and Toyota Motor Sales, U.S.A., Inc.*

10
11 UNITED STATES DISTRICT COURT
12 NORTHERN DISTRICT OF CALIFORNIA
13 SAN FRANCISCO DIVISION

14 HELENE CAHEN, KERRY J. TOMPULIS,
15 MERRILL NISAM, RICHARD GIBBS, and
LUCY L. LANGDON,

16 Plaintiffs,

17 v.

18 TOYOTA MOTOR CORPORATION,
19 TOYOTA MOTOR SALES, U.S.A., INC.,
20 FORD MOTOR COMPANY, GENERAL
MOTORS LLC,

21 Defendants.

CASE NO. 4:15-cv-01104-WHO

PUTATIVE CLASS ACTION

**DEFENDANTS TOYOTA MOTOR
CORPORATION AND TOYOTA MOTOR
SALES, U.S.A., INC.'S NOTICE OF MOTION
AND MOTION TO DISMISS PLAINTIFFS'
FIRST AMENDED COMPLAINT;
SUPPORTING MEMORANDUM OF POINTS
AND AUTHORITIES**

**REQUEST FOR JUDICIAL NOTICE AND
DECLARATION OF CHRISTINA YANG
FILED CONCURRENTLY**

Hearing

Date: November 3, 2015

Time: 3:00 p.m.

Courtroom: 2

The Hon. William H. Orrick

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION AND SUMMARY OF ARGUMENT	1
II. SUMMARY OF ALLEGED FACTS AND PROCEDURAL HISTORY	3
III. THE LEGAL STANDARDS GOVERNING THIS MOTION	7
IV. PLAINTIFF LACKS ARTICLE III STANDING TO PURSUE HER CLAIMS	8
A. Plaintiff Does Not Allege That She Experienced Any Vehicle “Hacking”	8
B. Courts Have Rejected Similar Attempts To Base Article III Standing On Hypothetical, Third-Party Criminal Conduct.....	10
C. Plaintiff Also Lacks Standing To Challenge Defendants’ “Data Collection” Practices, Because She Does Not Link That Alleged Conduct To Her Own Experience.....	13
V. THE STATUTES OF LIMITATIONS BAR ALL OF PLAINTIFF’S CLAIMS	13
VI. PLAINTIFF’S STATE LAW WARRANTY, FRAUD, AND INVASION OF PRIVACY CLAIMS FAIL AS A MATTER OF LAW	16
A. Plaintiff Does Not State, And Cannot Pursue, Any Warranty Claim	16
B. Plaintiff Also May Not Pursue Derivative Warranty Claims Through Her California Consumer Protection Or Fraud Claims	20
C. Plaintiff Does Not Allege A Sufficiently “Serious” Invasion To Support A Privacy Claim.....	22
VII. CONCLUSION	25

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Am. Suzuki Motor Corp. v. Super. Ct.</i> , 37 Cal. App. 4th 1291 (1995).....	19
<i>Asghari v. Volkswagen Grp. of Am., Inc.</i> , 42 F. Supp. 3d 1306 (C.D. Cal. 2013).....	14
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	7
<i>Banga v. Equifax Info. Servs., LLC</i> , No. 14-03038-WHO, 2015 WL 3799546 (N.D. Cal. June 18, 2015).....	23
<i>Bardin v. DaimlerChrysler Corp.</i> , 136 Cal. App. 4th 1255 (2006).....	20
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	7
<i>Belluomini v. Citigroup, Inc.</i> , No. 13-01743-CRB, 2013 WL 5645168 (N.D. Cal. Oct. 16, 2013).....	25
<i>Biden v. Common Cause</i> , 748 F.3d 1280 (D.C. Cir. 2014).....	11
<i>Birdsong v. Apple, Inc.</i> , 590 F.3d 955 (9th Cir. 2009).....	9, 13, 18, 19, 21
<i>Brooks v. Wash. Mut. Bank</i> , No. 12-00765-WHA, 2012 WL 5869617 (N.D. Cal. Nov. 19, 2012).....	14
<i>Cain v. State Farm Mut. Auto. Ins. Co.</i> , 62 Cal. App. 3d 310 (1976).....	14
<i>Chapman v. Pier 1 Imports (U.S.) Inc.</i> , 631 F.3d 939 (9th Cir. 2011).....	13
<i>Clapper v. Amnesty Int'l USA</i> , 133 S. Ct. 1138 (2013).....	8, 9, 11
<i>Clemens v. DaimlerChrysler Corp.</i> , 534 F.3d 1017 (9th Cir. 2008).....	15, 19, 20
<i>DaimlerChrysler Corp. v. Cuno</i> , 547 U.S. 3321 (2006).....	8, 11
<i>Daugherty v. Am. Honda Motor Co.</i> , 144 Cal. App. 4th 824 (2006).....	16, 20
<i>Doe v. Kaweah Delta Hosp.</i> , No. 08-118, 2010 WL 5399228 (E.D. Cal. Dec. 23, 2010).....	14

TABLE OF AUTHORITIES

(continued)

Page(s)

1		
2		
3	<i>Durkee v. Ford Motor Co.</i> ,	
4	No. 14-0617-PJH, 2014 WL 7336672 (N.D. Cal. Dec. 24, 2014).....	14
5	<i>Eclectic Prop. East, LLC v. Marcus & Millichap Co.</i> ,	
6	751 F.3d 990 (9th Cir. 2014).....	7
7	<i>Elias v. Hewlett-Packard Co.</i> ,	
8	950 F. Supp. 2d 1123 (N.D. Cal. 2013)	22
9	<i>Folgelstrom v. Lamps Plus, Inc.</i> ,	
10	195 Cal. App. 4th 986 (2011).....	24
11	<i>Fredenberg v. City of Fremont</i> ,	
12	119 Cal. App. 4th 408 (2004).....	24
13	<i>Frenzel v. AliphCom</i> ,	
14	76 F. Supp. 3d 999 (N.D. Cal. 2014)	7
15	<i>Hill v. Nat'l Coll. Athletic Ass'n</i> ,	
16	7 Cal. 4th 1 (1994)	23, 24
17	<i>Hovsepian v. Apple, Inc.</i> ,	
18	No. 08-5788-JF, 2009 WL 2591445 (N.D. Cal. Aug. 21, 2009).....	17
19	<i>In re Horizon Healthcare Servs., Inc. Data Breach Litig.</i> ,	
20	No. 13-7418, 2015 WL 1472483 (D.N.J. Mar. 31, 2015).....	12
21	<i>In re iPhone App. Litig.</i> ,	
22	844 F. Supp. 2d 1040 (N.D. Cal. 2012)	22, 24
23	<i>In re Toyota Motor Corp. Unintended Acceleration Litig.</i> ,	
24	754 F. Supp. 2d 1145 (C.D. Cal. 2010).....	17
25	<i>In re Yahoo Mail Litig.</i> ,	
26	7 F. Supp. 3d 1016 (N.D. Cal. 2014)	23
27	<i>Isaacs v. United States</i> ,	
28	No. 13-01394-WHO, 2013 WL 4067597 (N.D. Cal. Aug. 1, 2013)	7
	<i>Jones v. ConocoPhillips</i> ,	
	198 Cal. App. 4th 1187 (2011).....	20
	<i>Juniper Networks v. Shipley</i> ,	
	No. 09-0696-SBA, 2009 WL 1381873 (N.D. Cal. May 14, 2009)	15
	<i>Kearns v. Ford Motor Co.</i> ,	
	567 F.3d 1120 (9th Cir. 2009).....	8
	<i>Keilholtz v. Lennox Hearth Prods. Inc.</i> ,	
	No. 08-00836-CW, 2009 WL 2905960 (N.D. Cal. Sept. 8, 2009)	15

TABLE OF AUTHORITIES

(continued)

Page(s)

1		
2		
3	<i>Kirsopp v. Yamaha Motor Co.</i> ,	
4	No. 14-496, 2015 U.S. Dist. LEXIS 68639 (C.D. Cal. Jan. 7, 2015)	15
5	<i>Krottner v. Starbucks Corp.</i> ,	
6	628 F.3d 1139 (9th Cir. 2010).....	9, 12
7	<i>Lee v. Toyota Motor Sales, U.S.A., Inc.</i> ,	
8	992 F. Supp. 2d 962 (C.D. Cal. 2014).....	17, 21, 22
9	<i>Loder v. City of Glendale</i> ,	
10	14 Cal. 4th 846 (1997)	23
11	<i>Long v. Graco Children's Prods., Inc.</i> ,	
12	No. 13-01257-WHO, 2013 WL 4655763 (N.D. Cal. Aug. 26, 2013)	19
13	<i>Lujan v. Defenders of Wildlife</i> ,	
14	504 U.S. 555 (1992).....	8, 10, 11
15	<i>MacDonald v. Ford Motor Co.</i> ,	
16	37 F. Supp. 3d 1087 (N.D. Cal. 2014)	13
17	<i>Maya v. Centex Corp.</i> ,	
18	658 F.3d 1060 (9th Cir. 2011).....	11
19	<i>Morgan v. Harmonix Music Sys., Inc.</i> ,	
20	No. 08-5211, 2009 WL 2031765 (N.D. Cal. July 7, 2009).....	20
21	<i>Morning Star Packing Co. v. Crown Cork & Seal Co.</i> ,	
22	303 F. App'x 399 (9th Cir. Dec. 10, 2008).....	13
23	<i>Osborne v. Subaru of Am. Inc.</i> ,	
24	198 Cal. App. 3d 646 (1988).....	19
25	<i>Parker v. Iolo Techs., LLC</i> ,	
26	No. 12-00984, 2012 WL 4168837 (C.D. Cal. Aug. 20, 2012).....	13
27	<i>Peterson v. Mazda Motor of Am., Inc.</i> ,	
28	44 F. Supp. 3d 965 (C.D. Cal. 2014)	17
	<i>Pioneer Elec. (USA), Inc. v. Super. Ct.</i> ,	
	40 Cal. 4th 360 (2007)	22, 23
	<i>Public Citizen, Inc. v. NHTSA</i> ,	
	489 F.3d 1279 (D.C. Cir. 2007),	
	subsequent determination, 513 F.3d 234 (D.C. Cir. 2008)	9
	<i>Raines v. Byrd</i> ,	
	521 U.S. 811 (1997).....	13
	<i>Reilly v. Ceridian Corp.</i> ,	
	664 F.3d 38 (3d Cir. 2011).....	12

TABLE OF AUTHORITIES

(continued)

Page(s)

1		
2		
3	<i>Ries v. Arizona Beverages USA LLC,</i>	
4	287 F.R.D. 523 (N.D. Cal. 2012)	14
5	<i>Riva v. PepsiCo,</i>	
6	No. 14-02020-EMC, 2015 WL 993350 (N.D. Cal. Mar. 4, 2015)	10
7	<i>Seifi v. Mercedes-Benz USA, LLC,</i>	
8	No. 12-5439-TEH, 2013 WL 2285339 (N.D. Cal. May 23, 2013)	7, 14, 16
9	<i>Sharma v. BMW of N. Am., LLC,</i>	
10	No. 13-2274-MMC, 2015 WL 75057 (N.D. Cal. Jan. 6, 2015)	17
11	<i>Smith v. Ford Motor Co.,</i>	
12	462 F. App'x 660 (9th Cir. 2011)	21
13	<i>Smith v. LG Elecs. U.S.A., Inc.,</i>	
14	No. 13-4361-PJH, 2014 WL 989742 (N.D. Cal. Mar. 11, 2014)	17
15	<i>Storm v. Paytime,</i>	
16	No. 14-1138, 2015 WL 1119724 (M.D. Pa. Mar. 13, 2015)	10
17	<i>Taragan v. Nissan N. Am., Inc.,</i>	
18	No. 09-3660-SBA, 2013 WL 3157918 (N.D. Cal. June 20, 2013)	18, 19
19	<i>Tietsworth v. Sears, Roebuck & Co.,</i>	
20	720 F. Supp. 2d 1123 (N.D. Cal. 2010)	17, 21
21	<i>Troup v. Toyota Motors Corp.,</i>	
22	545 F. App'x 668 (9th Cir. 2013)	18
23	<i>U.S. Hotel & Resort Mgmt., Inc. v. Onity Inc.,</i>	
24	No. 13-1499, 2014 WL 3748639 (D. Minn. July 30, 2014)	12
25	<i>Vess v. Ciba-Geigy Corp. USA,</i>	
26	317 F.3d 1097 (9th Cir. 2003)	8
27	<i>Wasco Prods., Inc. v. Southwall Techs., Inc.,</i>	
28	435 F.3d 989 (9th Cir. 2006)	16
	<i>White v. Social Security Admin.,</i>	
	No. 14-05604-JST, 2015 WL 3902789 (N.D. Cal. June 24, 2015)	24
	<i>Wilson v. Hewlett-Packard Co.,</i>	
	668 F.3d 1136 (9th Cir. 2012)	20, 21
	<i>Xavier v. Philip Morris USA, Inc.,</i>	
	787 F. Supp. 2d 1075 (N.D. Cal. 2011)	20
	<i>Yumul v. Smart Balance, Inc.,</i>	
	733 F. Supp. 2d 1117 (C.D. Cal. 2010)	14, 15

TABLE OF AUTHORITIES
(continued)

Page(s)

<i>Yunker v. Pandora Media Inc.</i> , No. 11–03113–JSW, 2013 WL 1282980 (N.D. Cal.), and 2014 WL 988833 (N.D. Cal. Mar. 10, 2014).....	24
--	----

Constitutional Provisions

U.S. Const. art. III, § 2, cl. 1	8
Cal. Const. Art. I, § 1	6

Statutes

18 U.S.C. § 1030	11
Cal. Bus. & Prof. Code § 17200 <i>et seq.</i>	6
Cal. Bus. & Prof. Code § 17208	13
Cal. Bus. & Prof. Code § 17500 <i>et seq.</i>	6
Cal. Civ. Code § 1750 <i>et seq.</i>	6
Cal. Civ. Code § 1770(a).....	14
Cal. Civ. Code § 1783	13
Cal. Civ. Code § 1791.1(a)	18
Cal. Civ. Code § 1791.1(c)	17
Cal. Civ. Code §§1790-1795.8.....	6
Cal. Civ. Proc. Code § 335.1.....	14
Cal. Civ. Proc. Code § 337.....	13
Cal. Civ. Proc. Code § 338(d)	13
Cal. Com. Code § 2314.....	6, 13
Cal. Com. Code § 2314(2)(c).....	18
Cal. Com. Code § 2316(2)	17
Cal. Com. Code § 2725	13
Cal. Com. Code § 2725(2)	14
Cal. Penal Code § 502.....	11

TABLE OF AUTHORITIES
(continued)

Page(s)

Rules

Fed. R. Civ. P. 9(b)	7
----------------------------	---

Other Authorities

“Don’t Fret. It’s Still Really Hard To Hack Cars,” POLITICO (July 28, 2015), http://www.politico.com/morningtransportation/ 0715/morningtransportation19332.html	5
Andy Greenberg, “Hackers Remotely Kill A Jeep On The Highway—With Me In It,” WIRED (July 21, 2015), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/	5
Charlie Miller & Chris Valasek, “Adventures in Automotive Networks & Control Units,” http://illmatics.com/car_hacking.pdf	5
Chris Ingalls, “Smart apps pose privacy, security risks in some new cars” (May 20, 2015), http://www.king5.com/story/news/2015/05/19/ cars-auto-computer-security-hacking/27610967	5
Chris Valasek, “Lawsuit counterproductive for automotive industry,” http://blog.ioactive.com/2015/03/ lawsuit-counterproductive-for.html	6
Jim Travers, “Keeping Your Car Safe From Hacking,” CONSUMER REPORTS (May 7, 2015), http://www.consumerreports.org/cro/ news/2015/05/keeping-your-car-safe-from-hacking/index.htm	5
Jonathan Vanian, “Automakers unite to prevent cars from being hacked,” FORTUNE (July 14, 2015), http://fortune.com/2015/07/14/automakers-share-security-data	6
Stephen Checkoway, “Comprehensive Experimental Analyses of Automotive Attack Surfaces” (2011), http://www.autosec.org/pubs/cars-usenixsec2011.pdf	5, 9, 10
Xavier Aaronson, “We Drove a Car While It Was Being Hacked,” MOTHERBOARD (2014), <i>available at</i> http://motherboard.vice.com/read/we-drove-a-car-while-it-was-being-hacked ...	5, 10

1 TO THE COURT AND ALL PARTIES AND COUNSEL OF RECORD:

2 PLEASE TAKE NOTICE that on November 3, 2015, at 3:00 p.m., or as soon thereafter as
 3 they may be heard, in Courtroom 2 of this Court, located at 450 Golden Gate Avenue, San Francisco,
 4 California, before the Honorable William H. Orrick, Defendants Toyota Motor Corporation and
 5 Toyota Motor Sales, U.S.A., Inc. (collectively, “Toyota”) will and hereby do move the Court for an
 6 order dismissing all of the claims and causes of action contained in Plaintiff Helene Cahen’s First
 7 Amended Complaint pursuant to Rules 12(b)(1), 12(b)(6), and 9(b) of the Federal Rules of Civil
 8 Procedure. Toyota brings this Motion on the following grounds:

9 (1) Plaintiff Cahen’s purported “injury” rests on purely hypothetical, contingent, and
 10 conjectural allegations of harm that could only result from third parties’ criminal acts. Plaintiff’s
 11 allegations of some potential future alleged injuries are not the type of imminent, concrete, and
 12 particularized harms required for Article III standing.

13 (2) Even if this Court concluded that Plaintiff had standing to pursue her state law claims,
 14 the complaint still must be dismissed because all of her California warranty, fraud, consumer
 15 protection, and privacy claims are barred by the applicable statutes of limitations, which expired no
 16 later than 2012 (four years *after* she purchased her 2008 Lexus RX 400h, and more than two years
 17 *before* she filed this lawsuit).

18 (3) Separately, Plaintiff also fails to plead any claim for breach of warranty, fraud or
 19 deception, or invasion of privacy:

20 (a) Plaintiff cannot plausibly allege any claim for breach of warranty because:
 21 (i) any warranties applicable to her 2008 Lexus RX 400h expired by no later than September 2012;
 22 (ii) she does not identify any actionable statement, promise, or malfunction to support a claim for
 23 breach of express warranty; (iii) there are no allegations that her vehicle was not fit for its ordinary
 24 purpose of transportation, and therefore Plaintiff cannot pursue an implied warranty of
 25 merchantability claim under California law; and (iv) she also cannot pursue an implied warranty
 26 claim pursuant to binding Ninth Circuit precedent because she purchased her vehicle from a third-
 27 party dealer and thus lacks privity with Toyota.

28 (b) Plaintiff does not state a claim for fraudulent concealment or violations of

California's consumer protection/false advertising laws, because she cannot show that Toyota had any duty to disclose the alleged (and purely hypothetical) "defect," and she fails to satisfy Rule 9(b)'s heightened pleading standard applicable to fraud claims.

(c) Finally, Plaintiff cannot plausibly allege an invasion of privacy claim under the California Constitution because she has not alleged, and cannot amend her complaint to allege, either a *reasonable* expectation of privacy or the type of *serious* invasion of privacy required to maintain this claim.

STATEMENT OF ISSUES TO BE DECIDED PER CIVIL L.R. 7-4(A)(3)

1. Whether Plaintiff can establish Article III standing based on a theoretical possibility that her vehicle might be accessed unlawfully by criminals at some point in the future.

2. Whether the applicable statutes of limitations bar Plaintiff's California law claims relating to her 2008 Lexus RX 400h.

3. Whether Plaintiff may pursue a claim for breach of express or implied warranty given that any applicable warranties expired by their own terms more than two years ago, Plaintiff does not allege that she experienced any problems with her vehicle, and she lacks privity with Toyota.

4. Whether Plaintiff may pursue derivative warranty claims through her California consumer protection and/or common law fraud claims when Toyota had no legal duty to disclose the alleged hypothetical "defect," and when Plaintiff failed to plead her fraud claims with the particularity required under Rule 9(b) of the Federal Rules of Civil Procedure.

5. Whether Plaintiff's invasion of privacy claim must be dismissed because the complaint fails to allege either a reasonable expectation of privacy or the type of serious invasion of privacy required to maintain such a claim.

///

///

///

///

///

///

1 This Motion is based on this Notice of Motion, the attached Memorandum of Points and
2 Authorities; the accompanying Declaration of Christina Yang, Request for Judicial Notice, and
3 attached exhibits; the pleadings and papers on file in this action; and such other matters and argument
4 as may be presented to the Court at the time of the hearing on this Motion.

5
6 DATED: August 28, 2015

GIBSON, DUNN & CRUTCHER LLP

7 By: 
Christopher Chorba

8 *Attorneys for Defendants Toyota Motor Corporation*
9 *and Toyota Motor Sales, U.S.A., Inc.*

10 *Email: CChorba@gibsondunn.com*

I. INTRODUCTION AND SUMMARY OF ARGUMENT

Although the First Amended Complaint is a streamlined version of the original pleading (which was 343 pages long and alleged 238 separate claims arising under the laws of 50 states), it does not, and cannot, fix the underlying flaws in Plaintiffs' legal theory. Specifically, Plaintiffs base this putative class action on a speculative fear that someday, a very sophisticated cyber-criminal *might* be able to gain unlawful access to certain vehicles manufactured by Defendants Ford Motor Company, General Motors LLC, Toyota Motor Corporation, and Toyota Motor Sales, U.S.A., Inc.: "*if* an outside source, such as a *hacker*," were able to break into a Ford, GM, or Toyota vehicle, and gain "physical access" to the vehicle's Electrical Control Unit ("ECU"), then "the hacker *could* confuse one or more ECUs and . . . take control of basic functions of the vehicle away from the driver" (Pls.' First Am. Complaint [Dkt. 37] ("FAC") ¶¶ 4, 33 (emphases added)).

None of the Plaintiffs alleges that this criminal "hacking" has occurred to them, or that there is an imminent danger that an "attacker" will gain access to the controller access network ("CAN") bus units or ECUs inside their vehicles. Nor can Plaintiffs cite any actual, real-world incident in which any of the models of vehicles they own have been "hacked" (a point confirmed by the secondary sources cited in the complaint that report heavily controlled experiments). But Plaintiffs nonetheless seek to hold Defendants liable for the mere *possibility* of a high-tech criminal attack at some point in the future. This case is analogous to a lawsuit over a "data breach" before there has been any "breach," on the theory that a defendant's computer system *might* be vulnerable and *could* be attacked in the future. Plaintiffs' lawsuit thus represents the very type of "highly attenuated chain of possibilities" and "possible future injury" that the Supreme Court has rejected as insufficient to confer standing. Stretching Article III to accommodate this case would conflict with binding precedent and contravene the reasonable and sensible limitations enshrined in the United States Constitution.

Even if there were reports of a real-world, non-experimental incident in the vehicles that Plaintiffs own (and there are none), courts uniformly reject claims that seek preemptive redress for injuries that could only be caused (if at all) through the tortious and criminal acts of third parties. Plaintiffs' speculative theory of liability is not only contrary to precedent, it also defies common sense. Their claims are legally indistinguishable from the risk that vehicles may be subjected to other, non-

1 computerized acts of vandalism, such as tampering with the brakes, slashing the tires, smashing the
 2 headlights, or cutting the fuel line. That Defendants' vehicles (like any other product) are not
 3 completely invulnerable to destructive and illegal acts does not make them "defective," and the
 4 immutable fact that a vehicle cannot be designed to completely thwart all of the potential machinations
 5 of the criminal mind is hardly something for which Defendants can be liable.

6 Moreover, although the issues Plaintiffs identify have not arisen in real-world scenarios,
 7 vehicle manufacturers are mindful of the need to keep their proprietary technology secure, and they
 8 are working cooperatively with the responsible executive-branch regulators to proactively anticipate
 9 and address future threats. Those efforts are far more effective at stopping a hypothetical scenario
 10 from ever becoming a real one than a private class action based on a purely speculative injury.

11 Plaintiffs' lack of Article III standing disposes of this entire action, but all of the California
 12 state law claims by Plaintiff Helene Cahen—the only named plaintiff who purchased or leased a
 13 Toyota vehicle—are legally deficient for several additional and independent reasons:

14 First, all of Ms. Cahen's claims are barred by the applicable statutes of limitations. She
 15 purchased her Lexus RX 400h in September 2008, and she was required to bring all of her state law
 16 claims by no later than September 2012 (and earlier for her fraud and privacy claims). Plaintiff cannot
 17 circumvent the limitations barrier by asserting that Toyota somehow "misrepresented" or "failed to
 18 disclose" that a sophisticated criminal could tamper with the vehicle, as both state and federal courts
 19 repeatedly have rejected similar attempts to make manufacturers perpetual "guarantors" of their
 20 products. All of Plaintiff's claims are several years too late, she has not even attempted to meet her
 21 pleading burden to establish an exception to the statutes of limitations, and the Court should dismiss
 22 her claims with prejudice.

23 Second, Plaintiff cannot assert any express or implied warranty claim for several reasons:
 24 (a) any warranties applicable to her 2008 Lexus RX 400h expired by their plain terms more than two
 25 years ago (by no later than September 2012); (b) Plaintiff does not identify any actionable statement,
 26 promise, or vehicle malfunction to support her "common law" breach of warranty claim; (c) there are
 27 no allegations that her vehicle was not fit for its ordinary purpose of transportation, and therefore
 28 Plaintiff cannot pursue a claim for breach of the implied warranty of merchantability (either through

the Song-Beverly Act or Cal. Com. Code § 2314); and (d) she also cannot pursue an implied warranty claim because she purchased her vehicle from a third-party dealer and thus lacks privity with Toyota.

Third, Plaintiff cannot allege any derivative warranty claim based on either California consumer protection/false advertising statutes (Cal. Bus. & Prof. Code §§ 17200 or 17500) or common law “fraud by concealment,” because she cannot plausibly assert that Toyota had a legal duty to disclose the CAN bus unit’s alleged vulnerability to hacking. Plaintiff also fails to plead any of her statutory or common law fraud claims with the particularity required by Rule 9(b).

Fourth, the amended complaint does not state a plausible invasion of privacy claim under the California Constitution, because Plaintiff admits that the “data collection” practices were disclosed (and thus, she cannot claim that she had a reasonable expectation of privacy), and the alleged collection and transmittal of vehicle location data—even if true—does not constitute a sufficiently “serious” or “egregious” invasion to support this claim. Several courts in this District have rejected attempts to assert a constitutional privacy claim based on the alleged transmittal of geolocation data.

In sum, after taking two months to amend her pleading, Plaintiff Cahen still cannot plausibly assert a claim for relief. No future amendment can cure these fundamental legal deficiencies, and Toyota respectfully requests that this Court dismiss this action with prejudice.

II. SUMMARY OF ALLEGED FACTS AND PROCEDURAL HISTORY

Plaintiffs Kerry Tompulis, Merrill Nisam, and Helene Cahen filed a 343-page complaint on March 10, 2015, that asserted 238 claims against Defendants Ford Motor Company, General Motors LLC, Toyota Motor Corporation, and Toyota Motor Sales, U.S.A., Inc. (Compl. [Dkt. 1].) Plaintiffs alleged that the Electrical Control Units (ECUs) found in modern vehicles are “connected through a controller area network (‘CAN or ‘CAN bus’),” and that “[a]n attacker with physical access to a CAN bus-equipped vehicle could insert malicious code or CAN packets—and could also remotely and wirelessly access a vehicle’s CAN bus through Bluetooth connections.” (*Id.* ¶ 36.)

On April 30, 2015, Plaintiffs’ counsel informed Defendants that they were “consulting with experts and conducting further investigation,” and that they intended to amend the complaint. (*See* Joint Stip. [Dkt. 32] at 2; Order Granting Joint Stip. [Dkt. 33] at 1.) In their First Amended Complaint (“FAC”) filed on July 1, 2015 (Dkt. 37), Plaintiffs assert claims under California, Oregon, and

Washington law. They dropped 223 of their claims arising under federal law and the laws of other states, named two additional Ford owners as plaintiffs (but no new Toyota owners), and added a California invasion of privacy claim. But the central legal theory remains unchanged: Plaintiffs contend that Defendants’ vehicles are “defective” because there is a future possibility of “hacking.” (*Id.* ¶¶ 4, 8, 21, 26–28.) Specifically, they assert that “[t]he ECUs communicate by sending each other ‘CAN packets,’ which are digital messages containing data and/or requests,” and that “*if* an outside source, such as a *hacker*, were able to send CAN packets to ECUs on a vehicle’s CAN bus, the hacker *could* confuse one or more ECUs and thereby, either temporarily or permanently, take control of basic functions of the vehicle away from the driver.” (*Id.* ¶ 4 (emphases added).)

Plaintiff Cahen (the sole named plaintiff who owned or leased any Toyota vehicle) alleges that she purchased a new 2008 Lexus RX 400h from an authorized Lexus dealer in San Rafael, California, in September 2008. (*Id.* ¶ 12.) When Ms. Cahen purchased her vehicle, she received a limited warranty (*see* Compl. [Dkt. 1] ¶ 51) that covered any “repairs and adjustments needed to correct defects in materials or workmanship of any part supplied by Lexus” for 48 months or 50,000 miles (whichever occurred first). (*See* Def.’s Request for Judicial Notice (“RJN”), Ex. 1, at 17–19.) The warranty expressly disclaimed any guarantee against intrusion through “alteration or tampering,” and limited any implied warranties “to the duration of these written warranties.” (*Id.*)

Although Ms. Cahen (like her co-Plaintiffs) asserts that the CAN bus units on Toyota vehicles “are susceptible to hacking” (FAC ¶¶ 5, 8), she fails to allege that she has experienced any problems with her CAN bus unit or any other part of her vehicle. To the contrary, she concedes that she did not realize there could be anything allegedly “defective” with her vehicle “until shortly before this class action litigation was commenced” (*id.* ¶ 26), and the FAC continues to rely on secondary sources in which an unidentified vehicle was hacked under artificially-controlled conditions to demonstrate possible security vulnerabilities that could be exploited by sophisticated criminals (*id.* ¶¶ 28–39). Notably, none of these sources discussed an actual, non-experimental, incident despite widespread use of CAN-bus technology for more than a decade; the sources did not discuss Plaintiff Cahen’s vehicle (Lexus RX 400h); nor did these sources explain how an “attacker” could gain “physical” or “remote” access to the CAN bus unit outside of the conditions of a controlled experiment in which the vehicle

was made available to researchers attempting to “hack” the vehicle:

- The cited reports noted “the absence of any known attacks in the wild,” that widespread attacks “are highly speculative,”¹ and that the “possibilities seem more theoretical than practical at this point” (Chris Ingalls, “Smart apps pose privacy, security risks in some new cars” (May 20, 2015), *available at* <http://www.king5.com/story/news/2015/05/19/cars-auto-computer-security-hacking/27610967> (cited in FAC ¶ 15 n.3)).
- The FAC admitted that “[o]ne journalist described the experience of driving a vehicle whose CAN bus was being hacked remotely (but *under controlled circumstances*)” (FAC ¶ 35 (emphasis added).)
- Plaintiff cited a “Technical White Paper” in which a cable-connected laptop computer was used to gain physical access to the CAN bus units in *other* vehicles (a 2010 Toyota Prius and 2010 Ford Focus). (*Id.* ¶ 37 n.19 & n.20, citing Miller & Valasek, “Adventures in Automotive Networks & Control Units,” http://illmatix.com/car_hacking.pdf.)
- One article reported that to take control over vehicle functions “requires having a computer plugged into the car as well as having someone with an intimate knowledge of a car’s software system,” and that “remote access is not currently possible without having hardware that is hardwired into the car.” (Travers, “Keeping Your Car Safe From Hacking,” CONSUMER REPORTS (May 7, 2015), <http://www.consumerreports.org/cro/news/2015/05/keeping-your-car-safe-from-hacking/index.htm> (cited in FAC ¶ 40 n.24).)
- Another article quoted an information security researcher, who acknowledged that “[i]t is not easy to hack a car, the sophistication level is pretty high. Each car has a different language, each piece speaks different words, and not all those pieces have been mapped publicly.” (Xavier Aaronson, “We Drove a Car While It Was Being Hacked,” MOTHERBOARD (2014), *available at* <http://motherboard.vice.com/read/we-drove-a-car-while-it-was-being-hacked> (cited in FAC ¶ 35 n.17).)
- Another report confirmed the speculative nature of these attacks by emphasizing that, “in the *wrong hands*,” technical information “*could* also be used maliciously” and that the vehicles “*could be* compromised.” (FAC, Ex. 1 [Sen. Edward J. Markey Report, at 3 (2015)] (emphases added).) This report also did not identify any real-world incidents.²

¹ (Stephen Checkoway, “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” at 12–13 (2011), *available at* <http://www.autosec.org/pubs/cars-usenixsec2011.pdf> (cited in FAC ¶ 36 n.18) (hereinafter “Checkoway”).)

² An article that post-dated the filing of Plaintiffs’ FAC reported another highly-controlled experiment involving a vehicle (2014 Jeep Cherokee) that is not at issue in this lawsuit. (*See* Andy Greenberg, “Hackers Remotely Kill A Jeep On The Highway—With Me In It,” WIRED (July 21, 2015), *available at* <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.) The researchers who performed this experiment—“who had already devoted years to researching automotive security exploits—took months to discover the Jeep’s specific vulnerabilities,” which is “not the sort of investment malicious hackers are likely to make, especially when it would be much easier and cheaper to just cut an enemy’s brakes or put sugar in their gas tank.” (“Don’t Fret. It’s Still Really Hard To Hack Cars,” POLITICO (July 28, 2015), *available at* <http://www.politico.com/morningtransportation/0715/morningtransportation19332.html>.) Further, these researchers (Miller and Valasek) criticized this lawsuit as “unfortunate” and noted that it “subverts the spirit of our research.” (Valasek, “Lawsuit

[Footnote continued on next page]

1 This is not to say that the automobile industry is ignoring the potential threat of criminal
 2 intervention. Key industry stakeholders—including the Defendants in this case, nine other major
 3 automobile manufacturers, parts suppliers, and technology companies—have rallied together and
 4 established an information sharing and analysis center to share best practices on cybersecurity and
 5 subverting potential threats. (*See* Vanian, “Automakers unite to prevent cars from being hacked,”
 6 FORTUNE (July 14, 2015), *available at* <http://fortune.com/2015/07/14/automakers-share-security-data>.)

7 The FAC also alleges that Toyota collects and transmits data from Plaintiffs’ vehicles to third
 8 parties, “including but not limited to the geographic location of [her] vehicle[] at various times” (FAC
 9 ¶ 135), but Plaintiffs do not cite any specific practices by Toyota or how these practices impacted
 10 Plaintiff Cahen, and the FAC also concedes that “Defendants” disclosed these “data collection”
 11 practices in “owners’ manuals, online ‘privacy statements,’ and terms & conditions of specific feature
 12 activations.” (*Id.* ¶ 50.)

13 Although Plaintiff Cahen still cannot allege that any “hacker” ever gained “physical” or
 14 “remote” access to the CAN bus unit in her vehicle (or any other real-world incident in which anyone
 15 else’s vehicle was hacked), and she fails to identify the specific data that Toyota allegedly collected
 16 and transmitted from her 2008 Lexus RX 400h, she nonetheless asserts eight claims arising under
 17 California law on the ground that at some unknown point in the future, third parties *may* commit
 18 criminal acts involving her vehicle: (1) Unfair Competition Law (Cal. Bus. & Prof. Code § 17200 *et*
 19 *seq.*; “UCL”); (2) Consumers Legal Remedies Act (Cal. Civ. Code § 1750 *et seq.*; “CLRA”); (3) False
 20 Advertising Law (Cal. Bus. & Prof. Code § 17500 *et seq.*; “FAL”); (4) Implied Warranty of
 21 Merchantability (Cal. Com. Code § 2314); (5) Breach of Contract / Common Law Warranty;
 22 (6) Fraudulent Concealment; (7) Song-Beverly Consumer Warranty Act / Implied Warranty of
 23 Merchantability; and (8) Invasion of Privacy (Cal. Const. Art. I, § 1). (*Id.* ¶¶ 62–138.) Plaintiff seeks
 24 injunctive and monetary relief on behalf of a putative statewide class of “[a]ll persons or entities who
 25 purchased or leased a . . . Toyota Vehicle equipped with networked electronic or computerized

26 _____
 27 [Footnote continued from previous page]

28 counterproductive for automotive industry,” *available at* <http://blog.ioactive.com/2015/03/lawsuit-counterproductive-for.html>.)

components connected via a controller area network to an integrated cell phone or Class 1 or Class 2 master Bluetooth device in the State of California.” (*Id.* ¶ 51.)

III. THE LEGAL STANDARDS GOVERNING THIS MOTION

A complaint must be dismissed under Rule 12(b)(6) of the Federal Rules of Civil Procedure unless it “contain[s] sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). The court also may dismiss a complaint under Rule 12(b)(1) if the “plaintiffs do not carry their burden to allege facts which, if proved, would confer standing on them.” *Seifi v. Mercedes-Benz USA, LLC*, No. 12–5439–TEH, 2013 WL 2285339, at *2 (N.D. Cal. May 23, 2013); *Isaacs v. United States*, No. 13-01394-WHO, 2013 WL 4067597, at *1 (N.D. Cal. Aug. 1, 2013) (“If a plaintiff lacks standing . . . the district court has no subject matter jurisdiction.”).

Although courts must accept factual allegations as true for purposes of a motion to dismiss, this tenet is “inapplicable to legal conclusions.” *Iqbal*, 556 U.S. at 678; *see also Frenzel v. AliphCom*, 76 F. Supp. 3d 999, 1005 (N.D. Cal. 2014) (“Nor is the court required to accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences.”) (quoting *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008)). After stripping away the “conclusory statement[s]” in a complaint, the remaining factual allegations must do more than “create[] a suspicion of a legally cognizable right of action”; they must “raise a right to relief above the speculative level.” *Twombly*, 550 U.S. at 555, 561 (citation and quotations omitted); *Frenzel*, 76 F. Supp. 3d at 1005 (“[I]t is within [the court’s] wheelhouse to reject, as implausible, allegations that are too speculative to warrant further factual development.”) (quoting *Dahlia v. Rodriguez*, 735 F.3d 1060, 1076 (9th Cir. 2013)). In making this “context-specific” determination, a court must “draw on its judicial experience and common sense.” *Iqbal*, 556 U.S. at 679. This analysis provides a critical gatekeeping function, because claims must be sufficiently plausible such “that it is not unfair to require the opposing party to be subjected to the expense of discovery and continued litigation.” *Eclectic Prop. East, LLC v. Marcus & Millichap Co.*, 751 F.3d 990, 996 (9th Cir. 2014) (citation and quotation omitted).

In addition to these general pleading requirements, Rule 9 requires fraud-based claims to be pled with particularity. Fed. R. Civ. P. 9(b). As the Ninth Circuit explained, “[a]verments of fraud

must be accompanied by the ‘who, what, when, where, and how’ of the misconduct charged.” *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003). *See also Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125–27 (9th Cir. 2009) (applying Rule 9(b) to UCL and CLRA claims).

IV. PLAINTIFF LACKS ARTICLE III STANDING TO PURSUE HER CLAIMS

Plaintiff Cahen has failed to plead facts sufficient to establish that she suffered a cognizable “injury in fact” that satisfies “the irreducible constitutional minimum of standing” under Article III. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992); U.S. Const. art. III, § 2, cl. 1. To meet her burden, Plaintiff must allege more than a “highly attenuated chain of possibilities”; instead, as the Supreme Court has explained:

To establish Article III standing, an injury must be [1] “concrete, particularized, and actual or imminent; [2] fairly traceable to the challenged action; and [3] redressable by a favorable ruling.” “Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending.” Thus, we have repeatedly reiterated that “threatened injury must be *certainly impending* to constitute injury in fact,” and that “[a]llegations of *possible* future injury” are not sufficient.

Clapper v. Amnesty Int’l USA, 133 S. Ct. 1138, 1147–48 (2013) (emphases in original) (internal citations omitted); *see also DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 341 (2006) (“No principle is more fundamental to the judiciary’s proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies.”).

Plaintiff does not (and cannot) meet these requirements here, because she alleges a “highly attenuated chain of possibilities” that would occur only (if at all) as a result of sophisticated, third-party criminal conduct, *Clapper*, 133 S. Ct. at 1147, and she fails to allege any specific information about her own experience with “Defendants’” “data collection practices” (FAC ¶¶ 134–138).

A. **Plaintiff Does Not Allege That She Experienced Any Vehicle “Hacking”**

The complaint suffers from a fundamental, incurable defect: Plaintiff does not allege that any vehicle (let alone her vehicle) was “hacked,” nor does she allege any facts to plausibly demonstrate that she was at risk of being “hacked.” Instead, she alleges nothing more than the “possibility” that, at some point in the future, she *may* suffer harm because the CAN bus unit installed in her vehicle *may* be accessed unlawfully by a sophisticated third party: “*if* an outside source, such as a *hacker*, were

able to send CAN packets to ECUs on a vehicle’s CAN bus, the hacker *could* confuse one or more ECUs and thereby, either temporarily or permanently, take control of basic functions of the vehicle away from the driver.” (FAC ¶ 4 (emphases added).) **Nowhere in the 200 numbered paragraphs of the complaint is there *any* allegation that the CAN bus unit installed in Plaintiff Cahen’s 2008 Lexus RX 400h was hacked, or that she was harmed in any way.**

The Supreme Court has “repeatedly reiterated that ‘threatened injury must be *certainly impending* to constitute injury in fact,’ and that ‘[a]llegations of *possible* future injury’ are not sufficient.” *Clapper*, 133 S. Ct. at 1147. Likewise, the Ninth Circuit has consistently rejected attempts to base Article III standing on remote, conjectural, hypothetical, or speculative harms. For example, that court held that plaintiffs lacked Article III standing to pursue claims that the Apple iPod was “defective” because it “pose[d] an unreasonable risk of noise-induced hearing loss to its users.” *Birdsong v. Apple, Inc.*, 590 F.3d 955, 956, 960 n.4 (9th Cir. 2009). It explained that “[a]t most, the plaintiffs plead a potential risk of hearing loss not to themselves, but to other unidentified iPod users who might *choose* to use their iPods in an unsafe manner[,]” and therefore, “[t]he risk of injury the plaintiffs allege is not concrete and particularized *as to themselves*.” *Id.* at 960–61.

One year later, in *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010), the Ninth Circuit held that employees whose data was *stolen* had sufficiently alleged an increased risk of identity theft that was neither conjectural nor hypothetical, but “if no laptop had been stolen, and Plaintiffs had sued based on the risk that it *would be stolen at some point in the future*, [the court] would find the threat far less credible” and insufficient to establish Article III standing. Similarly, in a pre-*Clapper* decision, the D.C. Circuit rejected plaintiff’s theory of standing based on “an increased risk of death, physical injury, or property damage from *future car accidents* that [plaintiff] says NHTSA’s rule will fail to prevent.” *Public Citizen, Inc. v. NHTSA*, 489 F.3d 1279, 1293–94 (D.C. Cir. 2007), *subsequent determination*, 513 F.3d 234 (D.C. Cir. 2008).

In addition, none of the articles and secondary sources cited in the FAC demonstrates that there is an “imminent” and “real” threat that Plaintiff’s vehicle will be hacked. In fact, they illustrate the opposite by (1) expressly acknowledging “*the absence of any known attacks in the wild*” (Checkoway, *supra*, at 12-13); (2) recognizing that the likelihood of widespread attacks is “*highly*

1 *speculative*” (*id.*); (3) explaining that “it is *not easy to hack a car, the sophistication level is pretty*
 2 *high*” (*id.*); and (4) noting that the test vehicles were “*modified with third-party hardware*” because
 3 “[i]n stock form, [the car] is not vulnerable to these attacks” (Xavier Aaronson, “We Drove a Car
 4 While It Was Being Hacked,” MotherBoard, *available at* [http://motherboard.vice.com/read/we-drove-](http://motherboard.vice.com/read/we-drove-a-car-while-it-was-being-hacked)
 5 [a-car-while-it-was-being-hacked](http://motherboard.vice.com/read/we-drove-a-car-while-it-was-being-hacked) (2014) (see embedded video) (all emphases added)). One of these
 6 reports quotes a professor who observed, “[i]f you don’t have a risk of being assassinated normally,
 7 then you don’t have a risk of being assassinated from someone hacking your car. *If I just want to take*
 8 *you out, much easier to just shoot you.*” (*Id.*) Underscoring the point, one study repeatedly cautioned
 9 that its results were “*experimental*” (Checkoway, *supra*, at 15), and based on “*hypothetical*” scenarios
 10 (*id.* at 13) (emphases added).³ Notably, *none* of the cited sources involved the 2008 Lexus RX 400h.

11 By advancing a theory of injury that is based on nothing more than simulations demonstrating
 12 what a sophisticated criminal *might* do under controlled circumstances, Plaintiffs “have effectively
 13 invited the Court to engage in an ‘ingenious academic exercise in the conceivable to explain how
 14 defendants’ actions caused their injury.’” *Riva v. PepsiCo*, No. 14–02020–EMC, 2015 WL 993350,
 15 at *4, *14 (N.D. Cal. Mar. 4, 2015) (citation omitted). But theoretical, academic exercises cannot
 16 establish a threshold “injury in fact” that satisfies Article III. *See, e.g., Storm v. Paytime*,
 17 No. 14–1138, 2015 WL 1119724, at *6, *7 (M.D. Pa. Mar. 13, 2015) (rejecting plaintiffs’ attempt to
 18 establish Article III injury-in-fact, and noting that “courts cannot be in the business of prognosticating
 19 whether a particular hacker was sophisticated or malicious enough” to “engage in identity theft”). The
 20 Court should dismiss all of Plaintiff’s claims on this basis alone.

21 **B. Courts Have Rejected Similar Attempts To Base Article III Standing On Hypothetical,** 22 **Third-Party Criminal Conduct**

23 In addition to a concrete and particularized “injury in fact,” Plaintiff also fails to establish
 24 Article III standing because her speculative claims hinge on the future misconduct of third-party
 25 criminals. *See, e.g., Lujan*, 504 U.S. at 560 (the actual injury-in-fact must be “‘fairly . . . trace[able] to

26 ³ (*See also* FAC, Ex. 1, at 3 [Sen. Markey Report] (“Such information-gathering abilities *can* be used
 27 by automobile manufacturers to provide customized service and improve customer experiences, but in
 28 the *wrong hands* such information *could* also be used maliciously. In particular, wireless technologies
 create vulnerabilities to hacking attacks that *could* be used to invade a user’s privacy or modify the
 operation of a vehicle.”) (emphases added).)

the challenged action of the defendant, and not . . . the result [of] the independent action of some third party not before the court”). The Supreme Court recently “decline[d] to abandon [its] usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors.” *Clapper*, 133 S. Ct. at 1150; *see also id.* at 1150 n.5 (“[P]laintiffs bear the burden of pleading and proving concrete facts showing that the defendant’s actual action has caused the substantial risk of harm. Plaintiffs cannot rely on speculation about ‘the unfettered choices *made by independent actors not before the court.*’”) (emphasis added; quoting *Lujan*, 504 U.S. at 562). As the Ninth Circuit has explained, “[i]n cases where a chain of causation ‘involves numerous third parties’ whose ‘independent decisions’ collectively have a ‘significant effect’ on plaintiffs’ injuries, the Supreme Court and this court have found the causal chain too weak to support standing at the pleading stage.” *Maya v. Centex Corp.*, 658 F.3d 1060, 1070 (9th Cir. 2011) (citing *Allen v. Wright*, 468 U.S. 737, 757 (1984)). *See also Cuno*, 547 U.S. at 344 (holding that taxpayers lacked Article III standing because their claim depended on the future conduct of third-party actors in response to hypothetical events); *Biden v. Common Cause*, 748 F.3d 1280, 1285 (D.C. Cir. 2014) (holding that plaintiff lacked standing because the “alleged injury was caused not by any of the defendants, but by an ‘absent third party’”).

Here, any “harm” depends upon the future tortious and even **criminal** conduct that would violate a number of federal and state laws.⁴ Plaintiff apparently believes that vehicle manufacturers should be held liable *now* for alleged vulnerabilities that *might be* the subject of a criminal attack in the *future*. But the Ninth Circuit expressly rejected this very argument in *Krottner*. There, the court explained that although employees whose data had been *stolen* may satisfy Article III standing, the absence of any actual “theft” would render any injury speculative and non-actionable:

Were Plaintiffs-Appellants’ allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it **would be stolen at some point in the future**—we would find the threat far less credible.

⁴ *See, e.g.*, 18 U.S.C. § 1030 (Computer Fraud and Abuse Act; outlaws third-party hacking, such as “intentionally access[ing] a computer without authorization [] and thereby obtains [] information from any protected computer,” or “intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly causes damage”); Cal. Penal Code § 502 (Comprehensive Computer Data Access & Fraud Act; criminalizes third-party acts that “tamper[], interfere[], damage, and [provide] unauthorized access to lawfully created computer data and computer systems”).

628 F.3d at 1143 (emphasis added). That is precisely the theory offered by Plaintiff in this case—that an “attacker” “*could*” hack her vehicle at some point in the future. (FAC ¶ 4 (emphasis added).)

Other federal courts have rejected similar theories that depend on future criminal acts, including “hacking” or other sophisticated attacks. As the Third Circuit explained in *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), “we cannot now describe how [plaintiffs] will be injured in this case without beginning our explanation with the word ‘if’: *if* the hacker read, copied, and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully, only then will [plaintiffs] have suffered an injury.” *Id.* at 43 (emphases in original). And *U.S. Hotel & Resort Mgmt., Inc. v. Onity Inc.*, No. 13–1499, 2014 WL 3748639 (D. Minn. July 30, 2014), confronted a similar attempt by private plaintiffs to base Article III standing on hypothetical injuries that would occur in the future (if at all) only through the criminal intervention of third parties. In that case, an engineer published a study showing how to open hotel door locks using a homemade device. Several hotel owners brought a class action against the lock manufacturer, citing the future risk of unauthorized entry into the hotel rooms. But the District Court held that plaintiffs lacked Article III standing:

[T]he fact remains that no such unauthorized entry could occur unless and until that third party acted with *criminal intent* to gain entry. But where the future injury is contingent upon the actions of another, the Supreme Court has declined “to abandon [its] usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors” not before the court.

2014 WL 3748639, at *4 (quoting *Clapper*, 133 S. Ct. at 1150) (emphasis added). *See also In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, No. 13–7418, 2015 WL 1472483, at *6 (D.N.J. Mar. 31, 2015) (“Plaintiffs’ future injuries stem from the conjectural conduct of a third party bandit and are therefore inadequate to confer standing.”).

Plaintiff’s alleged injury—potential “hacking” of her vehicle—is speculative and entirely contingent upon the criminal acts of unknown third parties. Plaintiff’s claims are no different than a claim that a vehicle is “defective” because a criminal *might* cut the vehicle’s brake lines, slash its tires, smash the headlights, or throw a brick through the windshield. But this chain of “ifs” and “coulds” leads only to an independent third-party criminal actor, not Toyota. In sum, Plaintiff stands before the Court unharmed, and her speculative allegations of future injury that depend upon third parties’

criminal acts are legally insufficient to establish Article III standing.

C. Plaintiff Also Lacks Standing To Challenge Defendants’ “Data Collection” Practices, Because She Does Not Link That Alleged Conduct To Her Own Experience

Plaintiff’s “invasion of privacy” claim (FAC ¶¶ 132–138) also fails for lack of Article III standing. As the Supreme Court has held, private plaintiffs must establish that they have a “‘personal stake’ in the alleged dispute, and that the alleged injury suffered is particularized as to [themselves],” *Raines v. Byrd*, 521 U.S. 811, 819 (1997), and the Ninth Circuit consistently rejects attempts to base Article III standing on general allegations that are not specific to the plaintiffs, *see, e.g., Birdsong*, 590 F.3d at 961 & n.4; *Chapman v. Pier 1 Imports (U.S.) Inc.*, 631 F.3d 939, 954–56 (9th Cir. 2011).

Here, Plaintiff has pled nothing more than a generalized grievance that “Defendants” collected and transmitted unspecified “personal data” to unidentified third parties. (FAC ¶¶ 134–138.) She does not identify what “personal data” Toyota collected from her vehicle, what information Toyota shared with third parties, which third parties received the data, what those third parties did with the data, or any other facts that link the challenged practice to her own experience. In fact, Plaintiff concedes that she learned about this conduct because Defendants *disclosed* “such data collection in owners’ manuals, online ‘privacy statements,’ and terms & conditions of specific feature activations.” (*Id.* ¶ 50.) Plaintiff’s generalized grievances are legally insufficient to establish Article III standing. *See, e.g., Parker v. Iolo Techs., LLC*, No. 12-00984, 2012 WL 4168837, at *4 (C.D. Cal. Aug. 20, 2012) (rejecting general allegations that computer software did not work as advertised, because “Plaintiff does not plausibly allege that he suffered from these deficiencies of the software,” and thus he lacked standing). In any event, as discussed below, Plaintiff cannot pursue this claim because she has not established the necessary elements. (*Infra* pp. 22–25.)

V. THE STATUTES OF LIMITATIONS BAR ALL OF PLAINTIFF’S CLAIMS

All of the claims against Toyota fail for the independent reason that they are time-barred. Plaintiff’s claims are governed by two-, three-, or four-year statutes of limitations.⁵ Her claims

⁵ *See* Cal. Bus. & Prof. Code § 17208 (UCL—4 years); Cal. Civ. Code § 1783 (CLRA—3 years); Cal. Civ. Proc. Code § 338(d) (fraud—3 years); Cal. Com. Code § 2725 and *MacDonald v. Ford Motor Co.*, 37 F. Supp. 3d 1087, 1100 (N.D. Cal. 2014) (Song-Beverly Act/Cal. Com. Code § 2314/breach of implied warranties—4 years); Cal. Civ. Proc. Code § 337 and *Morning Star Packing Co. v. Crown Cork & Seal Co.*, 303 F. App’x 399, 402 (9th Cir. Dec. 10, 2008) (breach of contract—4 years); Cal.

[Footnote continued on next page]

1 accrued at the time of sale and tender of the vehicle—*i.e.*, when she purchased her Lexus RX 400h
2 vehicle in September 2008.⁶ Accordingly, the longest applicable statutes of limitations period
3 presumptively expired in September 2012, almost three years before Plaintiff filed this lawsuit.

4 In an attempt to avoid the obvious limitations bar, Plaintiff invokes the “delayed discovery
5 rule” and the “fraudulent concealment doctrine” (FAC ¶¶ 26–27), but neither exception applies here:

6 First, the delayed discovery rule cannot excuse Plaintiff’s delay in filing this action. As
7 another court in this District recently explained, “where applicable, [the delayed discovery rule]
8 postpones accrual of a cause of action until the plaintiff discovers, or has reason to discover, the
9 cause of action.” *Durkee v. Ford Motor Co.*, No. 14–0617–PJH, 2014 WL 7336672, at *6 (N.D. Cal.
10 Dec. 24, 2014). To delay the accrual of a cause of action under this rule, a plaintiff “must specifically
11 plead facts showing the time and manner of discovery and the inability to have made earlier
12 discovery despite reasonable diligence.” *Id.* Moreover, it is plaintiff’s burden to “show diligence,
13 and conclusory allegations will not withstand” dismissal. *Yumul v. Smart Balance, Inc.*, 733 F.
14 Supp. 2d 1117, 1130 (C.D. Cal. 2010) (quoting *E-Fab, Inc. v. Accountants, Inc. Servs.*, 153 Cal.
15 App. 4th 1308, 1319 (2007)). Here, despite the opportunity to further investigate and amend her
16 complaint, Plaintiff continues to offer only conclusory allegations that her claims should be tolled:

17 Any applicable statute(s) of limitations has been tolled by Defendants’ knowing

18 [Footnote continued from previous page]

19 Civ. Proc. Code § 335.1 and *Doe v. Kaweah Delta Hosp.*, No. 08–118, 2010 WL 5399228, at *13
20 (E.D. Cal. Dec. 23, 2010) (invasion of privacy—2 years). In addition, Plaintiff’s FAL claim is barred
21 by either the three-year limitations period in Cal. Code Civ. Proc. § 338(a) or the four-year limitations
22 period in the UCL. *Compare Ries v. Arizona Beverages USA LLC*, 287 F.R.D. 523, 534 (N.D. Cal.
2012) (“Claims under the [FAL] are governed by the three-year statute of limitations set forth in
California Code of Civil Procedure Section 338(a)”), with *Brooks v. Wash. Mut. Bank*, No. 12–00765–
23 WHA, 2012 WL 5869617, at *3 (N.D. Cal. Nov. 19, 2012) (applying UCL’s four-year statute of
limitations to FAL claim). Either way, this claim is time-barred.

24 ⁶ See Cal. Com. Code § 2725(2) (statute of limitations accrues upon tender of delivery); Cal. Civ.
25 Code § 1770(a) (a CLRA violation arises only in the context of a “transaction intended to result or
26 which results in the sale or lease of goods”); *Asghari v. Volkswagen Grp. of Am., Inc.*, 42 F.
27 Supp. 3d 1306, 1319 (C.D. Cal. 2013) (“Under the CLRA, the limitations period begins to run on the
28 date the improper consumer practice was committed.”); *Seifi*, 2013 WL 2285339, at *6 (“In this case,
the [Song-Beverly Act] cause of action on Plaintiffs’ implied warranty claims accrued, and the four-
year statute of limitations began to run, when the breach occurred, which was when tender of delivery
was made.”). See also *Cain v. State Farm Mut. Auto. Ins. Co.*, 62 Cal. App. 3d 310, 314 (1976)
 (“[T]he statute of limitations does not run [on a constitutional invasion of privacy claim] until the act
causing the [invasion] is discovered, or with reasonable diligence should have been discovered.”).

and active concealment and denial of the facts alleged herein. Plaintiffs and the other Class members could not have reasonably discovered the true, latent defective nature of the CAN buses until shortly before this class action litigation was commenced.

(FAC ¶ 26.) Because Plaintiff fails to allege the “time and manner of her discovery of the facts giving rise to her claims,” she cannot invoke the discovery rule to salvage her untimely claims. *See, e.g., Yumul*, 733 F. Supp. 2d at 1131 (holding that plaintiff’s “complaint does not plead sufficient facts to invoke the delayed discovery rule” because she failed to allege how she discovered the breach).

Second, for similar reasons, Plaintiff’s conclusory allegations are insufficient to invoke the “fraudulent concealment” doctrine. (*See* FAC ¶ 26 (“Any applicable statute(s) of limitations has been tolled by Defendants’ knowing and active concealment and denial of the facts alleged herein.”).) To invoke this exception, “plaintiff must show: (1) when the fraud was discovered; (2) the circumstances under which it was discovered; and (3) that the plaintiff was not at fault for failing to discover it or had no actual or presumptive knowledge of facts sufficient to put him on inquiry.” *Clemens v. DaimlerChrysler Corp.*, 534 F.3d 1017, 1024 (9th Cir. 2008) (internal quotations omitted). Plaintiff does not plead any of these elements here; she does not allege (1) **when** she discovered that her CAN bus unit was susceptible to hacking, (2) **how** she discovered the alleged “defect,” or (3) **why** she was not at fault for failing to discover it sooner. For these reasons, Plaintiff has failed to carry her burden and her claims should be dismissed. *See, e.g., Clemens*, 534 F.3d at 1024; *Yumul*, 733 F. Supp. 2d at 1133; *Keilholtz v. Lennox Hearth Prods. Inc.*, No. 08–00836–CW, 2009 WL 2905960, at *5 (N.D. Cal. Sept. 8, 2009).

Nor has Plaintiff satisfied the additional requirement of alleging “some active conduct by the defendant above and beyond the wrongdoing upon which the plaintiff’s claim is filed, to prevent the plaintiff from suing in time.” *Juniper Networks v. Shipley*, No. 09–0696–SBA, 2009 WL 1381873, at *5 (N.D. Cal. May 14, 2009) (internal quotations omitted); *Kirsopp v. Yamaha Motor Co.*, No. 14–496, 2015 U.S. Dist. LEXIS 68639, at *13–14 (C.D. Cal. Jan. 7, 2015) (holding that neither “failure to act” nor marketing representations constitute an “affirmative act of concealment on behalf of Defendant”). Once again, Plaintiff offers only vague and conclusory allegations of concealment (FAC ¶¶ 26–27) that fail to satisfy Rule 9(b). *See, e.g., Wasco Prods., Inc. v. Southwall Techs., Inc.*,

435 F.3d 989, 991 (9th Cir. 2006) (applying Rule 9(b) to allegations of “fraudulent concealment” designed to toll the statute of limitations).

Despite the opportunity for further amendment, Plaintiff continues to rely only on vague and conclusory allegations to toll her otherwise time-barred claims. These contentions are legally insufficient, and all of her warranty, fraud, statutory consumer protection, and invasion of privacy claims expired no later than September 2012 and are more than two years too late.

VI. PLAINTIFF’S STATE LAW WARRANTY, FRAUD, AND INVASION OF PRIVACY CLAIMS FAIL AS A MATTER OF LAW

In addition to the statute of limitations bar, all of Plaintiff’s claims fail for the alternate and independently sufficient reason that Plaintiff has not pled several essential elements to support her state law claims for breach of warranty, common law fraud, statutory consumer protection/false advertising, or invasion of privacy.

A. Plaintiff Does Not State, And Cannot Pursue, Any Warranty Claim

Plaintiff cannot pursue any claim for breach of warranty under California law (Counts IV, V, and VII) for several reasons:⁷

First, Plaintiff cannot maintain these claims because any warranties applicable to her 2008 Lexus RX 400h expired many years ago, and no later than September 2012. (RJN, Ex. 1 [express limited warranty covered 48 months or 50,000 miles, whichever occurred first].) The expiration of the limited express warranty bars any claim for an alleged post-warranty defect. *See, e.g., Daugherty v. Am. Honda Motor Co.*, 144 Cal. App. 4th 824, 830, 833 (2006) (rejecting attempt to require manufacturer to repair alleged defects “outside the limits of a written warranty”); *Seifi*, 2013 WL 2285339, at *4 (“[T]he warranty covers only those ‘repairs or replacements necessary’ as a result of something going wrong with the covered vehicle due to a defect within the specified time/mil[e]age limit. Since Plaintiffs do not allege that the defective gears failed during the warranty period, they have not stated a claim for breach of [Mercedes’] express warranty.”). Toyota also specifically limited

⁷ As an initial matter, it is unclear whether Plaintiff intends to assert an express or implied warranty claim through “Count V—Breach of Contract/Common Law Warranty.” (FAC ¶¶ 101–105.) The FAC dropped all of Plaintiff’s federal and state statutory express warranty claims (*see* Compl. [Dkt. 1] ¶¶ 65–76, 132–144), but whether or not Plaintiff intended to bring an express or implied warranty theory through Count V, it fails as a matter of law for the reasons discussed below. (*Infra* pp. 17–18.)

1 “[a]ny implied warranty of merchantability . . . to the duration of the[] written warranties” (RJN, Ex. 1,
 2 at 17), which is consistent with California law.⁸ Because Plaintiff purchased her 2008 Lexus RX 400h
 3 in September 2008 (FAC ¶ 12), any implied warranty would have expired no later than September
 4 2009. *See, e.g., Sharma v. BMW of N. Am., LLC*, No. 13–2274–MMC, 2015 WL 75057, at *4–5 (N.D.
 5 Cal. Jan. 6, 2015) (dismissing implied warranty claim “where the goods perform[ed] as warranted
 6 during the statutorily provided period and thereafter fail[ed] to continue to so perform”); *Peterson v.*
 7 *Mazda Motor of Am., Inc.*, 44 F. Supp. 3d 965, 972 (C.D. Cal. 2014) (holding that plaintiff must
 8 demonstrate that “her vehicle was unmerchantable *within* the implied warranty period set by the Song-
 9 Beverly Act in order to adequately plead a claim under the Song-Beverly Act”) (emphasis added).

10 Second, to the extent Plaintiff intends to assert an express warranty claim (*see supra* note 7),
 11 she cannot base this claim on Toyota’s description of its vehicles as “safe” in its marketing and
 12 promotional materials (FAC ¶¶ 41–44), because those descriptions do not include the type of “specific
 13 and unequivocal” statement necessary to create an express warranty. *In re Toyota Motor Corp.*
 14 *Unintended Acceleration Litig.*, 754 F. Supp. 2d 1145, 1182 (C.D. Cal. 2010); *see also Smith v. LG*
 15 *Elects. U.S.A., Inc.*, No. 13–4361–PJH, 2014 WL 989742, at *5 (N.D. Cal. Mar. 11, 2014) (“Vague
 16 statements regarding reliability, dependability, and *safety* are not actionable express warranties.”)
 17 (emphasis added). This claim also fails as a matter of law because Plaintiff does not even allege that
 18 she reviewed and relied upon these statements before purchasing her vehicle. *See, e.g., In re Toyota*
 19 *Motor Corp.*, 754 F. Supp. 2d at 1183 (dismissing warranty claim because plaintiffs failed to allege
 20 “they heard or read these statements or that the statements were otherwise disseminated to them”); *Lee*
 21 *v. Toyota Motor Sales, U.S.A., Inc.*, 992 F. Supp. 2d 962, 979 (C.D. Cal. 2014) (holding plaintiffs

22
 23 ⁸ *See* Cal. Civ. Code § 1791.1(c) (“The duration of the implied warranty of merchantability . . . shall
 24 be coextensive with an express warranty which accompanies the consumer goods[,] but *in no event*
 25 *shall such implied warranty have a duration of . . . more than one year* following the sale of new
 26 consumer goods to a retail buyer.”) (emphasis added); *Tietsworth v. Sears, Roebuck & Co.*, 720 F.
 27 Supp. 2d 1123, 1142 (N.D. Cal. 2010) (“The duration of an implied warranty of merchantability is one
 28 year if the express warranty is one year or more.”) (citing Cal. Civ. Code § 1791.1(c)); *Hovsepian v.*
Apple, Inc., No. 08–5788–JF, 2009 WL 2591445, at *7 (N.D. Cal. Aug. 21, 2009) (“In the absence of
 any indication in the statute that it is intended to supersede or extend Civil Code section 1791.1, we
 assume that [Cal. Com. Code] § 2314 does not extend the implied warranty . . . beyond the one year
 maximum contained in Civil Code section 1791.1.”); Cal. Com. Code § 2316(2) (authorizing the
 exclusion or modification of the implied warranty of merchantability).

could not base a claim on an express warranty created by statements in a marketing brochure, as they did “not allege that they read or relied on the ‘marketing brochure’ before making their purchases”). Nor does Plaintiff allege any “breach” by Toyota—she does not contend that her 2008 Lexus RX 400h was “unsafe,” that she had any problems with her vehicle, that she notified Toyota of any issues with her CAN bus unit, or that she sought any “repairs” pursuant to any warranty. As noted, Toyota’s express limited warranty covered 48 months or 50,000 miles (RJN, Ex. 1), and that warranty expressly disclaimed any damages resulting from “[a]lteration or tampering” (*id.* at 19), so Plaintiff cannot assert a preemptive “breach of warranty” claim based on a “hack” that has not yet occurred.⁹

Third, the Ninth Circuit has held that if a product is “fit for ordinary purposes for which such goods are used,” there is no breach of the implied warranty of merchantability. *Birdsong*, 590 F.3d at 958. *See also* Cal. Com. Code § 2314(2)(c) (“[T]o be merchantable,” goods “must be at least such as . . . [a]re fit for ordinary purposes for which such goods are used”); Cal. Civ. Code § 1791.1(a) (same). Here, Plaintiff cannot assert a claim for breach of the implied warranty of merchantability (Counts IV and VII) because she has failed to plead, and cannot plausibly amend her complaint to contend, that her vehicle was not fit for the ordinary purpose for which it was intended—namely, transportation. As another court in this District explained, “[i]n the case of automobiles, the implied warranty of merchantability can be breached only if the vehicle manifests a defect that is so basic it renders the vehicle unfit for its ordinary purpose of providing transportation.” *See, e.g., Taragan v. Nissan N. Am., Inc.*, No. 09–3660–SBA, 2013 WL 3157918, at *4 (N.D. Cal. June 20, 2013) (quoting *Am. Suzuki Motor Corp. v. Super. Ct.*, 37 Cal. App. 4th 1291, 1296 (1995)).

In *Taragan*, the plaintiffs alleged that Nissan’s vehicles were “not merchantable because there [was] a ‘risk’ that vehicles equipped with the Intelligent Key system [would] roll away if the operator fail[ed] to place the transmission in park after shutting off the engine.” 2013 WL 3157918, at *4. Notably, as in this case, “none of the Plaintiffs ha[d] actually experienced a rollaway incident” in

⁹ Nor can Plaintiff base any breach of an express warranty on an allegation that her vehicle’s CAN bus unit was defectively “designed” (*see, e.g.,* FAC ¶ 27), because elsewhere she admits that Toyota warranted only against defects in “materials or workmanship” (*id.* ¶ 103), and “[i]n California, express warranties covering defects in materials and workmanship *exclude defects in design.*” *Troup v. Toyota Motors Corp.*, 545 F. App’x 668, 668–69 (9th Cir. 2013) (emphasis added).

Taragan. Id. The court explained that “it is ***not enough*** to allege that a product line contains a defect or that a product is at risk for manifesting this defect; rather, the plaintiffs must allege that their product ***actually exhibited the alleged defect.***” *Id.* (emphases added). Similarly, Plaintiff merely alleges that a third party “could” engage in criminal conduct to “hack” her vehicle (FAC ¶ 4), but she does not allege that this has occurred. These allegations are legally insufficient. *See, e.g., Birdsong*, 590 F.3d at 959 (upholding dismissal of an implied warranty of merchantability claim because “plaintiffs do not allege the iPods failed to do anything they were designed to do nor do they allege that they, or any others, have suffered or are substantially certain to suffer inevitable hearing loss or other injury from iPod use”); *Am. Suzuki*, 37 Cal. App. 4th at 1298 (rejecting plaintiffs’ argument that “a remote fear or expectation of failure is sufficient to establish non-merchantability”).

Fourth, Plaintiff purchased her “new 2008 Lexus RX 400 H from an authorized Lexus dealer in San Rafael, California” (FAC ¶ 12), and thus she lacks privity with Toyota. As the Ninth Circuit has held, an “end consumer such as [plaintiff] who buys from a retailer is not in privity with a manufacturer,” and “[a] lack of vertical privity requires the dismissal of [plaintiff’s] implied warranty claims.” *Clemens*, 534 F.3d at 1023–24 (dismissing plaintiff’s implied warranty claim for lack of privity even though plaintiff purchased his vehicle from an “independent Dodge dealership”); *see also Osborne v. Subaru of Am. Inc.*, 198 Cal. App. 3d 646, 656 & n.6 (1988) (noting that California law requires vertical privity and holding that vehicle owners were foreclosed from recovering against manufacturer on an implied warranty of merchantability claim).

The FAC attempts to sidestep the privity requirement by alleging that Plaintiffs “are intended third-party beneficiaries of contracts between Defendants and their dealers; specifically, they are the intended beneficiaries of Defendants’ warranties.” (FAC ¶ 98.) But as this Court has held, the Ninth Circuit “does not recognize the [third-party beneficiary] exception under California law.” *Long v. Graco Children’s Prods., Inc.*, No. 13–01257–WHO, 2013 WL 4655763, at *12 (N.D. Cal. Aug. 26, 2013) (citing *Clemens*, 534 F.3d at 1024); *see also id.* (rejecting decisions purporting to create a “third-party beneficiary” exception, because they “are not binding on the Court whereas *Clemens* is”). As the Ninth Circuit explained, “California courts have painstakingly established the scope of the privity requirement under California Commercial Code section 2314, and a federal court sitting in

diversity is not free to create new exceptions to it.” *Clemens*, 534 F.3d at 1024.¹⁰

B. Plaintiff Also May Not Pursue Derivative Warranty Claims Through Her California Consumer Protection Or Fraud Claims

Next, Plaintiff asserts that Toyota violated the UCL, CLRA, and FAL (Counts I, II, III) and engaged in common law “fraud by concealment” (Count VI) by failing to disclose the alleged “defect” in its CAN bus system. (FAC ¶¶ 65(a), 81, 89, 111, 114.) Under binding California law, however, the omission of a fact that the defendant was not bound to disclose does not support a claim. *See, e.g., Daugherty*, 144 Cal. App. 4th at 839; *Morgan v. Harmonix Music Sys., Inc.*, No. 08–5211, 2009 WL 2031765, at *5 (N.D. Cal. July 7, 2009) (“[A]bsent a duty to disclose, the failure to do so does not support a claim under the fraudulent prong of the UCL.”); *Bardin v. DaimlerChrysler Corp.*, 136 Cal. App. 4th 1255, 1276 (2006) (rejecting plaintiff’s CLRA claim because the complaint did not allege facts showing that defendant was “bound to disclose” the allegedly concealed fact).

If Plaintiff seeks to base a claim on the alleged failure to notify customers of a supposed “defect,” she must allege that (1) the purported defect poses “an unreasonable safety hazard” and (2) the defendant “was aware of [the] defect *at the time of sale*.” *Wilson v. Hewlett-Packard Co.*, 668 F.3d 1136, 1142–43, 1145 (9th Cir. 2012) (emphasis added); *Daugherty*, 144 Cal. App. 4th at 835–36 (same). Both requirements are necessary to impose a legal duty on the defendant to disclose the alleged “defect,” *Wilson*, 668 F.3d at 1142–43, 1145–46, but Plaintiff cannot establish either of them:

First, the FAC contends that because Toyota “failed to ensure the basic electronic security of [its] vehicles, control of the basic functions of the vehicle can be taken by others not behind the wheel or necessarily even in the car, which can endanger the safety of the driver and others.” (FAC ¶ 2.)

Although Plaintiff alleges in a conclusory manner that the alleged “defect” presents a safety hazard

¹⁰ Plaintiff’s conclusory allegation that “privity is also not required because [her vehicle is a] dangerous instrumentalit[y] due to the aforementioned defects and nonconformities” (FAC ¶ 99) cannot excuse her from the privity requirement here. As an initial matter, she does not substantiate this far-fetched claim with any facts, and it is implausible that Plaintiff enjoyed the use of her vehicle for nearly seven years while it operated as a “dangerous instrumentalit[y].” Further, courts have explained that this limited exception applies to a defendant’s *employees*, not its customers. *See, e.g., Jones v. ConocoPhillips*, 198 Cal. App. 4th 1187, 1201 (2011) (“[T]he strict requirement of privity has also been excused when an inherently dangerous instrumentality causes harm to a buyer’s employee.”); *Xavier v. Philip Morris USA, Inc.*, 787 F. Supp. 2d 1075, 1083–84 (N.D. Cal. 2011) (noting that the “dangerous instrumentalities” exception to privity was limited to addressing “injur[ies] to an employee of the purchaser of the allegedly dangerous item”).

(*id.*), she alleges no real-world incident in which such a risk has ever manifested or is even likely to occur. An abstract and hypothetical risk does not trigger a “duty to disclose.”

For example, in *Birdsong*, Apple iPod users alleged that their portable music devices created a risk of hearing loss because there were no warnings or volume limits that kept the decibel levels at a safe range. The Ninth Circuit recognized that this was a potential risk in the abstract, but it nonetheless dismissed the plaintiffs’ UCL claim because “they [did] not claim that they, or anyone else, [had] suffered” the alleged injury. 590 F.3d at 961. Here, as in *Birdsong*, Plaintiff has failed to plead facts showing that “any identifiable member of the putative class actually experienced a malfunction” where the alleged safety consequences manifested. *Tietzworth*, 720 F. Supp. 2d at 1133–34. Instead, she merely alleges that “if an outside source, such as a hacker, were able to send CAN packets to ECUs on a vehicle’s CAN bus, the hacker could . . . take control of basic functions of the vehicle away from the driver.” (FAC ¶ 4 (emphases added).) These speculative fears are indistinguishable from a claim that a vehicle’s tires are dangerously “defective” because they are capable of being slashed, or that a windshield poses an “unreasonable safety hazard” because someone could maliciously shatter it with a baseball bat. The Ninth Circuit rejected another plaintiff’s attempt to use a speculative, future injury as sufficient to establish a “safety” issue:

Plaintiffs contend that the failure rate of the Focus ignition locks was related to safety because a defective lock may prevent the driver from starting the engine, thereby leaving the driver stranded on the roadway, or *may* prevent the engine from being shutoff, rendering the vehicle vulnerable to runaway or theft. We agree with the district court that the “safety” concerns raised by plaintiffs were ***too speculative***, as a matter of law, to amount to a safety issue giving rise to a duty of disclosure.

Smith v. Ford Motor Co., 462 F. App’x 660, 663 (9th Cir. 2011) (emphasis added). This is an even weaker case, because Toyota expressly *disclaimed* any warranty against vehicle intrusion: “This warranty does not cover damage or failures resulting directly or indirectly from any of the following: . . . ***Alteration or tampering***” (RJN, Ex. 1 at 19 (emphasis added).)

Second, Plaintiff does not contend that Toyota “knew of the alleged defect *at the time of sale*.” *Wilson*, 668 F.3d at 1148. Although she generally claims that Toyota knew about the alleged “defect” (FAC ¶¶ 5, 36), she does not identify a single fact to support that conclusory allegation (*see, e.g., Lee*, 992 F. Supp. 2d at 973 (rejecting plaintiff’s “conclusory allegations” as “insufficient”)) nor does she

1 allege that Toyota was aware of the purported problem *at the time of sale* in 2008 (*see Elias v.*
 2 *Hewlett-Packard Co.*, 950 F. Supp. 2d 1123, 1138 (N.D. Cal. 2013) (dismissing CLRA, UCL, and
 3 common law fraud claims because plaintiff “has not sufficiently alleged enough facts to support an
 4 inference that [defendant] knew of the power inadequacies at the time of sale” and as a result, he failed
 5 to allege that defendant “‘intentionally’ concealed or suppressed this information”).¹¹

6 Plaintiff’s “fraud by concealment” claim (Count VI) fails for the same reasons. As explained
 7 immediately above (*supra* pp. 20–22), Plaintiff cannot plead with particularity that Toyota had a “duty
 8 to disclose” the alleged “defect” because she cannot show that the problem materialized, that it poses
 9 an unreasonable safety hazard, *and* that Toyota knew about it *at the time of sale*. *See, e.g., Lee*, 992 F.
 10 Supp. 2d at 977; *Elias*, 950 F. Supp. 2d at 1136–37.

11 **C. Plaintiff Does Not Allege A Sufficiently “Serious” Invasion To Support A Privacy Claim**

12 Finally, Plaintiff’s “invasion of privacy” claim under the California Constitution (Count VIII;
 13 FAC ¶¶ 132–138) also fails as a matter of law. As the Supreme Court of California has explained,
 14 the constitutional “right of privacy protects the individual’s *reasonable* expectation of privacy against
 15 a *serious* invasion.” *Pioneer Elec. (USA), Inc. v. Super. Ct.*, 40 Cal. 4th 360, 370 (2007) (emphases
 16 added); *see also In re iPhone App. Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (“Actionable
 17 invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact
 18 to constitute an *egregious breach of the social norms* underlying the privacy right.”) (internal
 19 quotations and citation omitted; emphasis added). As one court explained, “[e]ven negligent conduct
 20 that leads to theft of highly personal information, including social security numbers, does not
 21 ‘approach [the] standard’ of actionable conduct under the California Constitution and thus does not
 22 constitute a violation of [a plaintiff’s] right to privacy.” *In re iPhone App. Litig.*, 844 F. Supp. 2d at
 23 1063 (quoting *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1128 (N.D. Cal. 2008)).

24
 25 ¹¹ Ms. Cahen’s only allegation regarding Toyota’s knowledge is conclusory, implausible, and post-
 26 dates the relevant time period (her 2008 purchase) by several years: “Before the researchers went
 27 public with their 2013 findings, they shared the results with Toyota and Ford in the hopes that the
 28 companies would address the identified vulnerabilities. The companies, however, did not.” (FAC
 ¶ 38.) Not only does Plaintiff fail to identify a single fact to support her conclusory allegation, but
 even if true, she bought her vehicle five years *before* the findings allegedly put Toyota on “notice” of a
 potential hacking risk. These pleaded facts foreclose any out-of-warranty UCL, FAL, or CLRA claim.

To state a claim for invasion of the constitutional right to privacy, Plaintiff must plead (and prove) three elements: “(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a *serious* invasion of privacy.” *Hill v. Nat’l Coll. Athletic Ass’n*, 7 Cal. 4th 1, 39–40 (1994) (emphasis added). These elements are intended to “weed out claims that involve *so insignificant or de minimis an intrusion* on a constitutionally protected privacy interest as not even to require an explanation or justification by the defendant.” *Loder v. City of Glendale*, 14 Cal. 4th 846, 893 (1997) (emphasis added).

Plaintiff’s conclusory allegations do not come close to meeting this high bar. For starters, her allegations do not even identify the specific “personal data” that Defendants allegedly “collected and transmitted to third parties.” (FAC ¶¶ 135–36.) This Court rejected a similarly conclusory “invasion of privacy” claim because the plaintiff did “not adequately allege[] what, if any, offensive and objectionable facts about her were disclosed to third parties.” *Banga v. Equifax Info. Servs., LLC*, No. 14–03038–WHO, 2015 WL 3799546, at *11 (N.D. Cal. June 18, 2015).

But even if Plaintiff overcame this hurdle, she cannot establish a “reasonable expectation of privacy” in the unspecified “personal data,” because she concedes that “Defendants” disclosed the alleged “data collection” practices (whatever they were) “in owners’ manuals, online ‘privacy statements,’ and terms & conditions of specific feature activations” (FAC ¶ 50.) *See, e.g., Hill*, 7 Cal. 4th at 42 (collegiate athletes had no reasonable expectation of privacy in the observation of their urination for purposes of drug testing, given previous disclosures of drug testing procedures at beginning of athletic season); *Pioneer*, 40 Cal. 4th at 372 (finding that plaintiffs, “having already voluntarily disclosed their identifying information to [defendant] in the hope of obtaining some form of relief, would [not] have a reasonable expectation that such information would be kept private”); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014) (rejecting generalized claim that plaintiffs had a “reasonable expectation of privacy” in all of their email messages).

Next, the FAC broadly identifies only two general categories of “personal data,” neither of which can support a claim for a “*serious* invasion of privacy.” *Hill*, 7 Cal. 4th at 40 (emphasis added). *First*, Plaintiff contends that Toyota and the other Defendants collected “the geographic location of [her] vehicle.” (FAC ¶ 135.) But sharing a vehicle’s location is not a “sufficiently

serious” invasion that would constitute “an *egregious* breach of the social norms underlying the privacy right.” *Hill*, 7 Cal. 4th at 37 (emphasis added). Courts in this District have ruled that the disclosure of location data does not constitute an “egregious” breach of social norms and is, therefore, legally insufficient to support an invasion of privacy claim. *See, e.g., In re iPhone App. Litig.*, 844 F. Supp. 2d at 1063 (holding that the disclosure to third parties of “unique device identifier number[s], personal data, and geolocation information” from plaintiffs’ cellphones did “not constitute an egregious breach of social norms” even if the information “was transmitted without [p]laintiffs’ knowledge and consent”); *Yunker v. Pandora Media Inc.*, No. 11–03113–JSW, 2013 WL 1282980, at *15 (N.D. Cal.) (holding that disclosure of plaintiffs’ personally identifiable information, including geolocation data, “to advertising libraries for marketing purposes” was insufficient to “allege that Pandora’s conduct constitutes an egregious breach of social norms”), and 2014 WL 988833, at *5 (N.D. Cal. Mar. 10, 2014) (dismissing amended right to privacy claim with prejudice “for the reasons set forth in its previous order”). Likewise, California courts have held that an individual’s location “is not the type of core value, informational privacy explicated in *Hill*.” *Fredenberg v. City of Fremont*, 119 Cal. App. 4th 408, 423 (2004); *see also Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011) (“Here, the supposed invasion of privacy essentially consisted of [defendant] obtaining plaintiff’s address without his knowledge or permission, and using it to mail him coupons and other advertisements. This is not an egregious breach of social norms, but *routine commercial behavior*.”) (emphasis added).

Second, Plaintiff also alleges that “[a]s detailed in Sen. Markey’s report, Defendants collect large amounts of data on driving history and vehicle performance, and they transmit the data to third-party data centers without effectively securing the data.” (FAC ¶ 50.) As an initial matter, the cited report does *not* identify which manufacturer engaged in this conduct, and Plaintiff does not allege that *Toyota* collected and/or shared “driving history and vehicle performance” data. (*Id.*) Without any specific allegation against Toyota that implicates a *serious* invasion, Plaintiff cannot meet her burden. *See, e.g., White v. Social Security Admin.*, No. 14–05604–JST, 2015 WL 3902789, at *7 (N.D. Cal. June 24, 2015) (holding that “unauthorized photocop[ying] of identity documents, without any allegation that [defendant] sold, distributed, or otherwise improperly used the information, does

not rise to the level of a ‘highly offensive disclosure of information nor a serious invasion of a privacy interest’”); *Belluomini v. Citigroup, Inc.*, No. 13–01743–CRB, 2013 WL 5645168, at *3 (N.D. Cal. Oct. 16, 2013) (rejecting claims that sharing of plaintiff’s “address and identity” stated an invasion of privacy claim, and reiterating earlier order that if the “disclosure of individual’s social security numbers does not constitute an ‘egregious breach,’ it certainly cannot be the case that disclosure of contact information constitutes an ‘egregious breach’”). Moreover, collecting “driving history and vehicle performance” (even if true) would not rise to the level of a “serious” invasion to support a constitutional privacy claim. (*Supra* pp. 23–24.)

VII. CONCLUSION

This action rests on a purely hypothetical, future injury that depends on the malicious acts of sophisticated criminals. Pursuant to binding Supreme Court and Ninth Circuit precedent, Plaintiff has not alleged sufficient “injury in fact” to satisfy Article III of the United States Constitution, and she may not cure this threshold problem with further amendment. On top of this threshold legal defect, Plaintiff’s California law claims are time-barred and her complaint fails to state any warranty, consumer protection, or invasion of privacy claim as a matter of law.

Toyota respectfully requests the Court dismiss this action with prejudice.

DATED: August 28, 2015

GIBSON, DUNN & CRUTCHER LLP

By: 
Christopher Chorba

101980989.11

*Attorneys for Defendants Toyota Motor Corporation
and Toyota Motor Sales, U.S.A., Inc.*

Email: CChorba@gibsondunn.com

CERTIFICATE OF SERVICE

I, Tiaunia Bedell, declare as follows:

I am employed in the County of Los Angeles, State of California, I am over the age of eighteen years and am not a party to this action; my business address is 333 South Grand Avenue, Los Angeles, CA 90071-3197, in said County and State. On August 28, 2015, I served the following document(s):

**DEFENDANTS TOYOTA MOTOR CORPORATION AND TOYOTA MOTOR
SALES, U.S.A., INC.'S NOTICE OF MOTION AND MOTION TO DISMISS
PLAINTIFFS' FIRST AMENDED COMPLAINT; SUPPORTING
MEMORANDUM OF POINTS AND AUTHORITIES**

on the parties stated below, by the following means of service:

Marc R. Stanley
Stanley Iola, LLP
3100 Monticello Avenue, Suite 750
Dallas, Texas 75205

Attorneys for Plaintiffs Helene
Cahen, Kerry J. Tompulis,
Merrill Nisam, Richard Gibbs,
and Lucy L. Langdon

Martin Darren Woodward
Stanley Law Group
6116 North Central Expy, Suite 1500
Dallas, TX 75206

Attorneys for Plaintiffs Helene
Cahen, Kerry J. Tompulis,
Merrill Nisam, Richard Gibbs,
and Lucy L. Langdon

Matthew J. Zevin
Stanley Law Group
10021 Willow Creek Rd, Suite 200
San Diego, California 92131

Attorneys for Plaintiffs Helene
Cahen, Kerry J. Tompulis,
Merrill Nisam, Richard Gibbs,
and Lucy L. Langdon

Donald H. Slavik
Slavik Law Firm, LLC
2834 Blackhawk Court
Steamboat Springs, Colorado 80487

Attorneys for Plaintiffs Helene
Cahen, Kerry J. Tompulis,
Merrill Nisam, Richard Gibbs,
and Lucy L. Langdon

Michael Mallow
Liv Kiser
Sidley Austin LLP
555 West Fifth St.
Los Angeles, California 90013

Attorneys for Defendant Ford
Motor Corporation

Gregory Oxford
Isaacs Clouse Crose & Oxford LLP
21515 Hawthorne Blvd, Suite 950
Torrance, California 90503

Attorneys for Defendant
General Motors LLC

Douglas Warren Sullivan
Crowell & Moring LLP
Embarcadero Center West
275 Battery Street, 23rd Floor
San Francisco, CA 94111

Attorneys for Defendant
General Motors LLC

Cheryl Adams Falvey
Kathleen Taylor Sooy
Rebecca Baden Chaney

Attorneys for Defendant
General Motors LLC

1001 Pennsylvania Avenue
Washington, DC 20004

☒ **BY UNITED STATES MAIL:** I placed a true copy in a sealed envelope or package addressed to the persons as indicated above, on the above-mentioned date, and placed the envelope for collection and mailing, following our ordinary business practices. I am readily familiar with this firm's practice for collecting and processing correspondence for mailing. On the same day that correspondence is placed for collection and mailing, it is deposited with the U.S. Postal Service in the ordinary course of business in a sealed envelope with postage fully prepaid. I am aware that on motion of party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing set forth in this declaration.

I am a resident or employed in the county where the mailing occurred. The envelope or package was placed in the mail at Los Angeles, California.

☒ **BY ELECTRONIC TRANSFER TO THE CM/ECF SYSTEM:** On this date, I electronically uploaded a true and correct copy in Adobe "pdf" format the above-listed document(s) to the United States District Court's Case Management and Electronic Case Filing (CM/ECF) system. After the electronic filing of a document, service is deemed complete upon receipt of the Notice of Electronic Filing ("NEF") by the registered CM/ECF users.

☒ I am employed in the office of Christopher Chorba, a member of the bar of this court, and that the foregoing document(s) was(were) printed on recycled paper.

☒ **(FEDERAL)** I declare under penalty of perjury that the foregoing is true and correct.

Executed on August 28, 2015.

/s/ Tiaunia Bedell

Tiaunia Bedell

101980989.11